Marco Pivetta
(Ocramius (//twitter.com/Ocramius))

YubiKey for SSH, Login, 2FA, GPG and Git Signing

I've been using a YubiKey Neo (https://www.yubico.com/products/yubikey-hardware/yubikey-neo/) for a bit over two years now, but its usage was limited to 2FA (Two Factor Authentication) and U2F (Universal Two Factor Authentication).

Last week, I received my new DELL XPS 15 9560, and since I am maintaining some high impact open source projects, I wanted the setup to be well secured.

In addition to that, I caught a bad flu, and that gave me enough excuses to waste time in figuring things out.

In this article, I'm going to describe what I did, and how you can reproduce my setup for your own safety as well as the one of people that trust you.

Yubi-WHAT?

In first place, you should know that I am absolutely not a security expert: all I did was following the online tutorials that I found. I also am not a cryptography expert, and I am constantly dissatisfied with how the crypto community reduces everything into a TLA (Three Letter Acronym), making even the simplest things impossible to understand for mere mortals.

First, let's clarify what a YubiKey is.

That thing is a YubiKey.

What does it do?

It's basically an USB key filled with crypto features. It also is (currently) impossible to make a physical copy of it, and it is not possible to extract information written to it.

It can:

- Generate HMAC (Hash Message Authentication Code) hashes (kinda)
- Store GPG (Gnu Privacy Guard) private keys
- Act as a keyboard that generates time-based passwords
- Generate 2FA time-based login codes